Foundation of Cryptography, Spring 2014 Iftach Haitner

Problem set 4

May 27, 2014 Due: In class – June 10. By email – June 12.

- Please submit the handout in class, or email me, in case you write in LaTeX
- Write clearly and shortly using sub claims if needed. The emphasize in most questions is on the proofs (no much point is writing a “solution" w/o proving its correctness)
- For Latex users, a solution example can be found in the course web site.
- In it ok to work in (small) groups, but please write the id list of your partners in the solution file, and each student should write his solution by *himself* (joint effort is only allowed in the “thinking phase")
- The notation we use appear in the introduction part of the first lecture (*Notation* section).

1. Let $(\mathsf{G}, \mathsf{E}, \mathsf{D})$ be an encryption scheme that has indistinguishable encryptions in the private-key model. Assume that $\operatorname{Supp}(\mathsf{G}(1^n)) \subseteq \{0,1\}^n \times \{0,1\}^n$, and that on $(e, \cdot) \in \operatorname{Supp}(\mathsf{G}(1^n))$ and $m \in \{0,1\}^{2n}$, algorithm $\mathsf{E}_e(m)$ uses at most $\ell(n)$ random bits. Let $\mathsf{E}_e(m; r)$ denote the output of $\mathsf{E}_e(m)$ whose random coins are set to r.

   Prove that the function f over $\{0,1\}^n \times \{0,1\}^{2n} \times \{0,1\}^{\ell(n)}$, defined by

   $$f(e, m, r) = (\mathsf{E}_e(m; r), m),$$

   is a (partial-domain) one-way function.

2. Consider the following variant of construction 19 in Lecture 8 (Encryption Lecture).

   Let (G_T, f, Inv) be a (non-uniform) TDP, and let b be hardcore predicate for it.

   Construction 1 (bit encryption)**.**

   - $\mathsf{G}(1^n)$*: output* $(e, d) \leftarrow \mathsf{G}_T(1^n)$.
   - $\mathsf{E}_e(m)$*: choose* $r \leftarrow \{0,1\}^n$ *conditioned that* $b(r) = m$*, and output* $f_e(r)$ *(output* m *if no such* r *exists).*
   - $\mathsf{D}_d(y)$*: output* $b(\mathrm{Inv}_d(y))$.

   (a) Describe a PPT E' such that $\Pr_{(e,d)\leftarrow\mathsf{G}(1^n); m\leftarrow\{0,1\}}[\mathsf{E}'_e(m) \neq \mathsf{E}_e(m)] \leq \operatorname{neg}(n)$.

   (b) Prove that $(\mathsf{G}, \mathsf{E}', \mathsf{D})$ has public-key indistinguishable encryptions for a multiple messages.

3. Assume we change Algorithm 30 in Lecture 8 so that j is Step 1 is always set to 0 (rather than being chosen at random). Is Claim 31 still true?